FAQ

FORTINET INTERNAL USE ONLY – Do Not Distribute

FortiAP Technical FAQ

Technical FortiAP Frequently Asked Questions

Access Point Questions

Can I power the outdoor FAP-222B with a regular 802.3af PoE injector?

A regular 802.3af PoE injector (for example, the Fortinet GPI-115) only provides up to 15.4 Watts of power. Due to the high power output of the FAP-222B access point, 802.3at PoE+ is required, which provides up to 25.5 Watts of power.

See the table below for a full list of the power supply requirements for each FAP:

	Power Supply Type	Power supply shipped with unit	(Spare) Power supply order SKU	GPI-115 Support
FAP-11C	AC	Yes - Integrated power plug	-	-
FAP-14C	AC	Yes	-	-
FAP-28C	AC	Yes	-	-
FAP-112B	PoE Proprietary	Yes - Proprietary PoE injector and AC adaptor	-	-
FAP-210B	PoE 802.3af	Yes	SP-FAP220B-PA-<Country Suffix>	Yes
FAP-220B	PoE 802.3af	Yes	SP-FAP220B-PA-<Country Suffix>	Yes
FAP-221B/223B	PoE 802.3af	No	SP-FAP221B-PA + SP-ADAPTORPLUG-01-<Country Suffix>	Yes
FAP-221C	PoE 802.3af	No	SP-FG20C-PA-<country suffix>	Yes
FAP-222B	PoE 802.3at/POE Proprietary	Yes - Proprietary PoE+ injector and AC adaptor	SP-FAP222B-PA (includes PoE injector) + SP-ADAPTORPLUG-01-<Country Suffix>	-
FAP-320B	PoE 802.3af	No	SP-FG20C-PA-<country suffix>	Yes
FAP-320C	PoE 802.3af	No	SP-FG20C-PA-<country suffix>	Yes

How do I perform a factory reset on an FAP?

If you know the password, you can telnet to the FAP and type `factoryreset` at the command prompt.

If you do not know the password, there are a two different ways to perform a factory reset on an FAP, depending on the FAP model.

To perform a factory reset via the factory reset button:

- FAP-210B and FAP-220B - The reset button is not labeled, but is located through one of the ventilation holes on the bottom side of the FAP. The ventilation hole is the top raw second hole from the right. Insert a paper clip to press the reset button and the unit will factory reset and reboot.

- FAP-221B, FAP 221C and FAP-223B - The reset button is not labeled, but is located through the individual hole above the FORTINET logo on the front face of the FAP. Insert a paper clip to press and hold the reset button for 7-10 seconds until the power LED blinks orange.

- FAP-320B and FAP320C - The reset button is labeled, and is located close to the LAN1 Ethernet port on the side wall of the FAP. Insert a paper clip through the hole to press and hold the reset button for 5-7 seconds. Once reset, you need to manually power cycle the FAP. If you hold the reset button for less than 5-7 seconds, the AP will reboot but will not reset the configuration back to factory default.

- FAP-222B - There is no reset button on the FAP-222B, however there is a reset button on the power injector. Press and hold the reset button on the power injector for 10 seconds.

- FAP-11C- The reset button is not labeled, but is located in the front side through the individual hole below the LEDs are. Insert a paper clip to press and hold the reset button for around 7 seconds until the LEDs start blinking again.

A picture of the reset button location on most APs can be found in the quick-start guide that comes with the unit, or from http://docs.fortinet.com.

To perform a factory reset via a firmware flash through the console port:

On the FAPs with a console port (FAP-210B, FAP-220B FAP-320B and FAP-320C), you can connect to the FAP through the console and flash a new firmware version to it via TFTP to reset the configuration back to factory default.

To perform the firmware flash, connect the console cable before powering the FAP. When ask to interrupt the booting sequence, press any key, then type “G” and provide the IP address of the TFTP server, the local address to use on the FAP, and the file name for the FAP firmware package.

What is the coverage area of each Fortinet AP?

It is not possible to provide a general expectation of coverage area for an AP. Detailed information on the environment and the performance expectations is required to provide realistic expected coverage area values.

There are many factors that determine the size of the coverage area for a given frequency, including:

- Obstructions between the AP and the station that can create attenuation, reflections and other propagation alterations.
- Station sensitivity for the different data rates (based on the type of client, antenna gain, and technology).
- Bandwidth expectations or requirements inside the coverage area.

- Station transmit power output back to the AP

As the data rate or modulation rate depend on the signal strength, and the signal decreases with distance, the further the station is from the AP the slower data rates the station will be able to demodulate. A coverage area that allows you to maintain a session at 150Mbps is significantly smaller than the coverage area at 1Mbps for example.

For a non obstructed line of sight environment, such outdoors, once you know the Access Point transmit power you can get a quick estimation of the signal level at different distances. With this information, you can then determine the possible Data Rates for a particular station. Remember that any WiFi connection is a bi-directional and that also in the upstream direction the client needs to be able to reach the AP. The coverage area will also be heavily impacted by the device with the least transmit power and gain.

When I upgrade the wireless controller, are the FAPs also upgraded?

No. The FortiGate Wireless Controller and FAPs must be upgraded independently. There are many situations where you only want to upgrade one component and not the other. For example, there may be version compatibility requirements, or small fixes in the FAP that don't require a full controller upgrade.

What is the hop limit in a Fortinet wireless mesh network?

There is no hard limit to the number of hops in a Fortinet wireless mesh network. The realistic hop limit depends on the network utilization and traffic requirements. Multiple hops can cause bottlenecks in the network, so the overall hop count needs to be managed carefully to ensure the network performance meets the customer's needs. However, it is important to note that by default, the maximum hop value is set to 4. This parameter can be changed in every AP with the variable MESH_MAX_HOPS if more hops are required.

How many users can a single FAP handle?

There is no hard limit to the number of users a single FAP can handle. The realistic number of users a single FAP can handle depends on the radio design, as well as the application and the bandwidth requirements. A single 802.11n AP with a 2x2 radio design can realistically handle up to 70Mbps of TCP traffic using 20MHz channels, and around 140Mbps using bonded 40Mbps channels.

This means that the number of users per radio could vary from 3-5 in the case of a direct wire replacement, to over 100 in cases of wireless telemetry or credit card transactions. It is also important to keep in mind that beyond certain number of users, the limiting design factor could be signal and coverage, rather than number of users per radio.

To assess the realistic number of users that a single FAP can handle, it is first important to understand how much bandwidth is required per user. From here, you can apply an oversubscription rate, as well as compensate for non ideal environments (20-30% less than the theoretical maximum in most cases). This should then give you an estimate of the number of users that a single FAP radio can handle.

Some examples of the realistic number of users per radio are:

- 3-7 - For a direct wire replacement.
- 8-15 - In high VoIP environment, high performance enterprise, significant video, etc.
- 16-25 - Average high bandwidth enterprise and schools with 1:1 deployments, some video.
- 26-50 - Hot spots and events, where you need basic connectivity, email and web browsing.
- >50 - Low bandwidth applications, credit card transactions, barcode readers, telemetry, etc.

The user experience may also depend of other environmental factors, such as the number of other APs in the vicinity using the same RF channel, the level of general RF interference, and whether the 2.4GHz or 5GHz band is used.

Do other wireless vendors handle more users per AP?

The number of users that can be handled per AP are very similar across all vendors, as this is an RF channel and wireless standard limitation. Performance may be slightly different however, depending on each vendor's capability to optimize the rating algorithm, signal, and sensitivity.

A significant differentiator in the Fortinet wireless solutions is the ability to shape bandwidth and/or block traffic on a very granular per application or user basis, in addition to the Single Sign On features. The low cost of adding APs to existing Fortigate customers is also a significant differentiator, reducing the TCO for a customer even if the FAP may handle fewer users per AP over a competitor product.

When should I use the FAP-221B versus the FAP-223B?

One of the key differences between the FAP-221B and the FAP-223B is that the FAB-223B has external antennas. The standard external antennas of the FAB-223B have a higher gain than the internal antennas of the FAP-221B, providing a slightly larger coverage area. In scenarios where wider coverage is more important than density or capacity, and aesthetics are not necessarily important, you may want to consider the FAP-223B instead of the FAP-221B. Theoretically, due to the larger coverage area of the FAP-223B, fewer APs can be used to cover a given area, providing a lower TCO in some environments. If external antennas are required for any other reason in a given scenario, the FAP-223B is the access point to use.

It is important to note that both antenna patterns are still omnidirectional (or quasi), however the FAP-223B has an antenna pattern on more of a horizontal pane than vertical. Moreover, since you can re-orient the antennas on the FAP-223, you have some flexibility in the antenna pattern.

When it comes to higher capacity and user dense environments, the FAP-221B is a better option as in many cases, as the goal will be to reduce the cell size to optimize for user capacity, rather than extended coverage. This means that the FAP-221 will generally be the product to lead with, where as the FAP-223B will be used in specific scenarios, such as those mentioned above, where extended coverage or external antenna capabilities are required.

From a competitive perspective, some wireless vendors have similar models of AP with both external and internal antenna capabilities: for example, the Aruba 104/105, or the Aruba 134/135. This means that in some cases the choice to recommend the FAP-221B or the FAP-223B may be more to do with the customers' expectation, or our competitor's recommendation, rather than a genuine technical reason.

Which FAP models have spectrum analysis capabilities?

The following FAP models have a chipset that can perform spectrum analysis and can also identify sources of non-WiFi interference: FAP-14C, FAP-28C, FAP-221B, FAP-223B and FAP-320B.

What type of external antenna connectors are on the Fortinet FAPs?

- FAP-222B - N-type female
- FAP-223B - RP-SMA female

What are the two CAPWAP UDP ports that FortiGate Controller and FAPs use to communicate?

- Control channel - UDP 5246
- Data channel - UDP 5247

These port numbers can be changed, however they must still be 2 consecutive port numbers.

Is IPv6 supported with FortiAPs?

Yes. IPv6 is supported in FortiAP and FortiGate. There are two scenarios where only IPv4 is currently supported: Mesh and SSIDs configured in Local Bridge mode. Additionally, IPv6 address won't be displayed in the wireless GUI, or logs but IPV6 traffic will passes through FAPs and FortiGate.

Can I limit the number of wireless clients that can connect to a FAP?

Yes. There are three places to configure the maximum number of clients, each with a different scope.

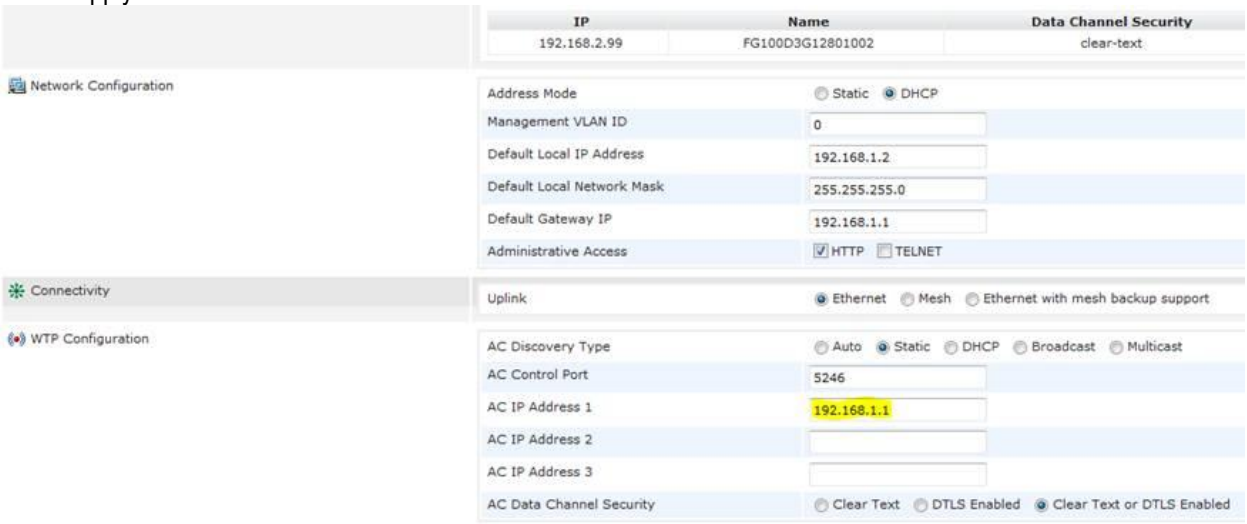
- `config wireless-controller wtp-profile`
  - This setting configures the maximum number of wireless stations supported by the WTP. This is a per radio setting.
- `config wireless-controller vap (SSID)`
  - This setting configures the maximum number of wireless stations supported for a specific SSID across all FAPs.
- `config wireless-controller global`
  - This setting configures the maximum number of wireless stations supported by the entire FortiGate Wireless Controller.

How do I provision a remote FAP to be managed by a centralized Wireless Controller?

Remote FAPs can be provisioned via a HTTP GUI or a Telnet CLI, if Telnet has is enabled on the FAP.

To provision via the HTTP GUI:

1. Connect the FAP to the network and allow it to obtain an IP address from DHCP.
2. Connect to the IP address of the FAP using HTTP. If there is no DHCP server on the network, the default IP address of the FAP will be 192.168.1.2
   - Username: admin, no password.
3. Ensure that the FAP is running the correct firmware version for your environment. If the firmware is not correct, upgrade it at this point.
4. On the main page under network configuration is recommended to leave the IP address mode as DHCP so they FAP gets the appropriate IP for the remote site and the correct default gateway.
5. On the WTP configuration, set the AC IP address 1 to the IP address of the centralized controller (see the screenshot below).
6. Click apply to finish.



To provision via the Telnet CLI:

1. Ensure Telnet is enabled.
   - When the unit is not authorized by a controller, Telnet is enabled. Once the unit has been authorized by a controller, it becomes disabled unless you re-enable it. Telnet can be re-enabled on the FAP via the HTTP interface.
2. Connect the FAP to the network and allow it to obtain an IP address from DHCP.
3. Connect to the IP address of the FAP using Telnet. If there is no DHCP server on the network, the default IP address of the FAP will be 192.168.1.2
   - Username: admin, no password.
4. Ensure that the FAP is running the correct firmware version for your environment. If the firmware is not correct, upgrade it at this point.
5. Type the following commands to configure the AC IP Address:

```
cfg -a AC_DISCOVERY_TYPE=1
cfg -a AC_IPADDR_1=192.168.1.1
cfg -c  (To commit changes to flash)
```

For site survey purposes, can I use an FAP to broadcast an SSID without having a controller?
Yes. To configure the FAP to broadcast an SSID without a controller, simply Telnet to the FAP that you want to use for the survey and set the variable AP_MODE=2 and save the configuration. The FAP will then reboot and start broadcasting an SSID called "FAP_SURVEY" by default.

For example:

```
cfg -a AP_MODE=2
cfg -c
```

The following variables can be set manually for site survey purposes:

- `SURVEY_SSID='FAP_SURVEY'`
  - This setting configures the SSID that will be broadcast.
- `SURVEY_TX_POWER=30`
  - This setting configures the TX power of the FAP. By default, this is configured at 30dBm (which is the maximum TX power of any FAP). Some FAPs however transmit at a maximum power of 17dBm however.
- `SURVEY_CH_24=6`
  - This setting configures the TX channel for the 2.4Ghz band. By default, this is configured as channel 6.
- `SURVEY_CH_50=36`
  - This setting configures the TX channel for the 5Ghz band. By default, this is configured as channel 36.
- `SURVEY_BEACON_INTV`

Can I configure and SSID to provide wireless LAN access directly on the FAP, without using a controller?
No. You can only configure an SSID directly on the FAP for site survey purposes. The SSID configuration settings for wireless LAN access come from the controller via the wtp-profile.

If the controller is down, can the AP still receive new client connections and maintain the existing ones?
Yes. In FortiOS version 5.0.3 and later, the FAP will still operate when the controller is not reachable. This is applicable for SSIDs configured in Bridge mode (not tunneled to the controller) and with security settings set to Open or WPA/WPA2 PSK.

What is multicast optimization?
In wireless networks, multicast traffic is generally treated in the same way as broadcast traffic, where the lowest data rate available is used, and no frame acknowledgement is required. This can make multicast transmissions slow and unreliable.

One way to improve the performance of multicast traffic is to convert the traffic stream from multicast to unicast. In doing this, the most optimal data rate for each station will be used and fames will also benefit from improved reliability through frame acknowledgement.

To enable multicast optimization on an SSID, the following options can be set from the CLI console:

- `set multicast-enhance enable|disable`
  - This setting enables or disables multicast conversion.
- `set me-disable-thresh value`
  - This setting creates a threshold so that no multicast-to-unicast conversion occurs if the number of wireless stations belonging to a multicast group becomes too large.

Why can't I see custom AP profiles in my FortiGate GUI?

In certain FortiGate models, such as the FG-40C, the Custom profiles are not visible in the GUI by default.

To enable custom profiles in the GUI on these models, configure the following:

```
config system global
```

and

```
set gui-ap-profile enable.
```

FortiGate Wireless Controller Questions

Can I use FTGT-VM with a 15 day evaluation license as a wireless controller?

The free 15 day evaluation license does not support any wireless controller features.

All of the wireless features are supported in the employee evaluation license (365 days) and customer evaluation license (60 days).

How many FAPs can a single FTGT-VM appliance manage?

As of January 2013, the maximum number of FAPs supported on each of the FTGT-VM appliances is:

- FG-VM00 - 32
- FG-VM01 - 256
- FG-VM02 - 512
- FG-VM04 - 512
- FG-VM08 - 1024

Wireless Authentication Questions

Can I use client certificate authentication with local user groups in the in the FortiGate?

When using local user groups, WPA Enterprise mode does not support client certificate authentication, such as EAP-TLS. WPA Enterprise mode only supports server certificate authentication using EAP-PEAP.

Client certificate authentication is supported when Fortigate is acting as the authenticator and authenticates against an external RADIUS server.

Can I use 802.1x to authenticate users against LDAP, without a RADIUS server?

The FortiGate Wireless Controller can be used as an 802.1x authenticator and authentication server without the need for an external RADIUS server (this is known as Local EAP). In this case however, the authentication occurs against local user groups only (therefore users need to be defined locally on the FortiGate), and can't authenticate users against an external LDAP server.

An alternative solution is to configure the Fortigate to use an external RADIUS sever that authenticates users against an LDAP database, such as a Microsoft Network Policy and Access Services (NPS) server in Windows 2008.

Can I use a peer user (PKI) for wireless EAP authentication?

No. A PKI, or peer user, is only used for firewall and VPN authentication. PKI user authentication can be achieved by using EAP-TLS authenticating against an external RADIUS server.

What EAP authentication methods are supported when using local user groups?

When using WPA/WPA2 Enterprise with local user groups, only the EAP-PEAP authentication mode is supported. By default, the FortiGate is loaded with a server certificate valid for 10 years for this purpose.

What EAP authentication methods are supported when using an external RADIUS server?

The following authentication methods are supported on the FortiGate Wireless Controller using an external RADIUS server:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- EAPv0/EAP-MSCHAPv2
- PEAPv1/ EAP-GTC
- EAP-SIM,
- EAP-AKA
- AP-FAST

Captive Portal Questions

How do I set a disclaimer only page?

1. Create an SSID and configure it with the Captive Portal security mode, ensure that there are no user groups defined against the SSID.
2. Create a firewall policy, set the Captive Portal SSID as the Incoming Interface and set the other conditions as required.
3. Set disclaimer to enable via the CLI.

For example:

```
edit 1
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set disclaimer enable
    set nat enable
```

How do I set an E-mail harvesting collection portal?

An E-mail Collection Portal prompt is configured via a tick-box in a device identity policy.

How do I control the timeout of a Captive Portal user?

Captive Portal timeout configuration is performed from the CLI console. This can be set at a global level, which will apply to all users and groups, or at a group level, which will apply only to the User Group you specify.

To set a timeout globally:

```
config user setting
set auth-timeout <number_minutes>
set auth-timeout-type {idle-timeout | hard-timeout | newsession}
end
```

To set a timeout on a specific user group:

```
config user group
edit <group>
set authtimeout <number_minutes>
end
```

How do I redirect the Captive Portal to another external page?

In the Captive Portal page HTML code, insert the following HTML code between the “head” tags:

```
<meta http-equiv="Refresh" content="5; url=http://the_other_page ">
```